INFORMATION ATTACK

IW 160

OPR: Captain Gerry Eisert

DESCRIPTION: This lesson discusses the Information Warfare pillar, Information Attack.

METHODOLOGY: Informal Lecture/1.25 Hours

COGNITIVE OBJECTIVE: The objective of this lesson is for each student to comprehend the basic concepts of information attack.

COGNITIVE SAMPLES OF BEHAVIOR:

1. Identify how the AF defines an Information Attack and the two different types.
2. Identify the Military and the Non-Military Threat of an Information Attack
3. Identify the indicators of an information attack and how to recognize them.
4. Explain how Information Attack supports Information Warfare.
5. Explain what the AF can do to protect our Information Systems against such an attack.

AFFECTIVE OBJECTIVE: The objective of this lesson is for each student to respond positively to the concept of information attack as a pillar of information warfare.

AFFECTIVE SAMPLES OF BEHAVIOR:

1. Effectively discuss how the components of information attack could enhance the warfighter
2. Positively participate in examples of Information Attack
3. Discuss positively the environment in which information attack exists.
4. Willingly reply to questions asked by lecturer on the information attack.

REQUIRED READINGS:

1. *Joint Chiefs Inaugurate Information Combat Era by George I. Seffers, Defense News, Instructional Circular pages 160-H-1 through 160-H-2.*

2. *Hacker Awareness, Instructional Circular pages 160-H-3 through 160-H-12.*

Joint Chiefs Inaugurate Information Combat Era

By George I. Seffers, Defense News Staff Writer

WASHINGTON -- In a move military experts say is the start of the new information-age era in military conflict, the U.S. Joint Chiefs of Staff are adopting a new doctrine for conducting computer warfare. For the first time, offensive computer network attacks will become an intrinsic part of U.S. warfighting doctrine, and even could be used in peacetime operations. Experts say the implications are staggering. This "will go down in history as the start of the information operations arms race. The publication of the 'Joint Doctrine for Information Operations' shatters, or rather redefines, the illusion of peace," William Church, an information operations expert who publishes "CIWARS [Center for Infrastructural Warfare Studies] Intelligence Report," an Internet newsletter, said Nov. 4. "To put it bluntly, it is now official. Each country must build offensive-defensive information operations capabilities or be left unprotected."

The Joint Chiefs of Staff soon will send to regional commanders "Joint Doctrine for Information Operations," the first official doctrine to explain the U.S. military's strategy and operational concepts for information warfare.
The document covers computer network attacks as one part of so-called information operations, which the Joint Chiefs define also as including operations security, military deception, psychological operations, electronic warfare, physical attack and destruction, and special information operations. The doctrine paper includes newly defined terminology for computer- based warfare, a move experts welcomed as helping ensure that military leaders are in sync.

For example, information warfare, a more common term often used interchangeably with information operations, is defined more narrowly as information operations conducted during times of conflict or crisis. "Offensive [information operations] may be conducted in a variety of situations and circumstances across the range of military operations and may have their greatest impact in peace and the initial stages of a crisis.... Offensive information operations may be conducted at all levels of war -- strategic, operational, and tactical -- throughout the battlespace," says the document, signed Oct. 9 by Army Gen. Hugh Shelton, chairman of the Joint Chiefs of Staff.

Pentagon officials insist they will consider international laws, treaties and agreements before conducting computer network attacks. "Information operations, including computer network attacks, involve many complex legal and policy issues that require national-level coordination and approval. Broad areas that must be considered include domestic and international criminal and civil laws affecting national security, privacy and information exchange, as well as international treaties and agreements," Lt. Cmdr. Jim Brooks, a spokesman for the Joint Chiefs of Staff, said Nov. 5. Some experts noted, however, that there are no treaties covering computer attacks.

Robert Clyde, an executive at Axent Technologies Inc., an information security company based in Rockville, Md., said Nov. 5 the document puts other countries on notice the

United States is willing and able to conduct offensive information operations. "It definitely serves notice to all other countries in the world that this is something the [United States] is going to do," Clyde said. "It is similar to the Star Wars announcement back in the 1980s, in purpose if not in scope. It certainly sounds like the U.S. [military] might engage in some activities that could be considered acts of war." Clyde and others said integrating information operations into military doctrine is a necessary step, especially since countries such as China already have made it clear they intend to do the same.

Integrating computer network attacks into joint doctrine, some experts say, means the Pentagon has developed the capability to a degree that it can be used reliably.
"We've had the capability to do this for a long time, but we've never come out with an actual doctrine for it," Anderson Wilkerson, president of ARIES (Advanced Research in Information and Engineering Systems) Technology Corp., Dumfries, Va., said Nov. 4. "This is basically saying that anything goes in a peacetime setting." Wilkerson, a former Air Force official who worked with the National Security Agency, said the U.S. military conceivably could use information operations, namely cyber attacks, in its traditional policy of escalating pressure on potential adversaries. The United States could opt, for example, to disable another country's electric power source or communications centers before launching a physical attack. "This gives us a different set of options for responding to a multilateral threat. The implications are really huge, especially in developing countries like North Korea or Iraq," he said. Church said the document shows the military has come a long way in its understanding of information operations, and that offensive network attacks offer an advantage that no longer can be gained through conventional weapons widely available in the aftermath of the Cold War.

"The core issue is that information operations is a weapon of mass destruction, and we need to face that fact. When you map infrastructures right, combine that with good intelligence, combine that with good simulation programs coupled with command and control software, then you can design an approach that will destroy a nation," Church said. The new doctrine now is available on the Internet, with the exception of a classified section detailing computer network attack issues. The unclassified section does address some of the issues surrounding offensive information operations, including strategic, operational and tactical targeting.

Defense News November 9-15, 1998

~ HACKER AWARENESS ~

White House Commission Studying ATC Vulnerability to Hacker Attacks

Another White House commission may soon be making recommendations that impact the Air Traffic Control (ATC) system. The President's Commission on Critical Infrastructure Protection is studying the vulnerability of "critical infrastructure" to interference by external agents and is expected to list hacker attacks against the ATC system as one of the threats in a new global era of information warfare.

Information warfare is divided into two schools of thought. The first predicts large scale calamities if drastic, and expensive actions, are not taken to protect the U.S. information infrastructure from attackers. This type of information warfare is often referred to as the Electronic Pearl Harbor.

The second school of information warfare takes a less apocalyptic view. Supporters of this view believe that the nation's computer infrastructure is so redundant and fault tolerant that the possibility of hackers causing widespread damage is remote. What is the threat to ATC systems? The ATC system is said to be most vulnerable to hacker attacks where the ground-to-pilot communications are routed through the telephone system, because their switching systems are a favorite target of amateur computer hackers.

For example, a group of teenagers crashed New York City's Con Ed Power Company in 1995 by attacking the telephone company's Manhattan switch. The individuals achieved access to the system by searching through telephone company trash cans looking for passwords - not by a technologically advanced maneuver.

"So far, hackers have shown little morbid interest in crashing the ATC. The worst we have to worry about is an `Oops!' from the ATC itself more than hackers," says Winn Schwartau, an information security consultant and author.

A full-scale information warfare assault against the U.S. would not just affect the ATC system. A realistic assault probably would also target banking, electric power grids, ground traffic management, telecommunications systems, the water system and defense and warning systems.

Global Positioning Systems (GPS) and Loran are particularly vulnerable to hackers. GPS is notoriously jammable using simple equipment that can be purchased at auto parts or technology stores. Loran data travels via the telephone switching systems but has built-in protections against telephone outages. The weakness of the GPS system has created a new type of threat called "navigational warfare" where opponents try to disrupt each other's GPS systems.

However, there have been no serious attacks as of yet. "To date, we have found no evidence of cyber attack on the (ATC) infrastructure," said William Church, editor of The Journal of Infrastructure, a publication which tracks hacker attacks.

The President's Commission on Critical Infrastructure Protection reportedly has a spotty record. The Commission was slow to get started after the Defense Department failed to sign on in 1995. Additionally, the commission has a low level of computer industry involvement, which troubles some industry executives. The commission is scheduled to report its findings in October.

AIR SAFETY WEEK, Vol.11 Issue 27

Cyberfraud

Today, most banking is done by electronic impulse, surpassing cheques and cash by a wide margin. In the near future, nearly all business transactions will be electronic. Thus, access to business computers equals access to money.

Recently, computer hacker John Lee, a founder of the infamous `Masters of Deception' hacker group, discussed his 10-year career, which began when he was 12 years old and included a one-year prison term in his late teens. Without admitting to any wrongdoing, Lee said that he could "commit a crime with five keystrokes" on the computer. He could: (1) change credit records and bank balances; (2) get free limousines, airplane flights, hotel rooms, and meals "without anyone being billed", (3) change utility and rent rates; (4) distribute computer software programmes free to all on the Internet; and (5) easily obtain insider trading information. Though prison was "no fun," Lee admitted that he would certainly be tempted to do it all again.

In a groundbreaking study published in Criminal Justice Review in the spring of 1994, Jerome E Jackson of the California State University reported the results of a study of a new group of criminals he called "fraud masters". These professional thieves obtain credit cards via fake applications, or by electronic theft, and pass them around among their peers internationally for profit. These young men and women want the "good life" after growing up in poverty. They are proud of their skills of deception and arrogant enough to feel they won't be caught. Indeed, none of those in the five-year case study were caught.

As seen in the $50-million-plus losses in the MCI case, a far greater threat to businesses than hackers are disgruntled and financially struggling employees. As internal theft from retail stores has always been many times greater in volume than theft from shoplifters, robbers, and burglars, theft by employees armed with inside information and computer access is and will continue to be a much larger problem than intrusion by hackers, crackers, and terrorists combined.

In addition, the future portends new and brighter `for-profit' invasion of business computers. As one US justice department official warns, "This technology in the hands of children today is technology that adults don't understand." The first generation of computer-literate citizens will reach adulthood shortly after the turn of the century and will surely open a new age in the annals of crime and crime fighting.

- Gene Stephens in The Futurist.

TIMES OF INDIA 22/07/97

Hacker Breaks Into State Web Page Again

The Minnesota Department of Public Safety is investigating the second break-in to the state's web page in less than two weeks.

The incident occurred early Wednesday and blocked access to the public e-mail system. The Internet news service Channel 4000 reports there are indications the latest incident may have been the work of the same hacker who deleted a day's worth of files and posted a cryptic message 10 days ago.

Elaine Hansen, commissioner of the Minnesota Department of Administration, says the initial attack was the first security breach since the state launched its "North Star" web site two years ago.

Hansen told Channel 4000, "I think it's very unfortunate. If we want to have the freedom of the Internet to be able to access a great deal of information, we're going to have to install some type of encryption and
hopefully it will not deter people from using the Internet."

United Press International.

Hackers Devastate Texas Newspaper's Servers

By Levins, Hoag

THE SAN ANTONIO Express-News' Web site server systems were severely damaged by a hack-attack in mid-April, according to a company official who addressed an opening day Nexpo New Media workshop in New Orleans. Although scheduled to give a relatively dry technical speech about how to set up and operate equipment for an Internet Service Provider (ISP) business, Express-News online managing editor Jon Donley revealed that his newspaper's ISP, as well as eight other regional ISPs, suffered major hack-attacks seven weeks ago.

He said none of the other eight ISP companies have publicly acknowledged being hacked and that the newspaper had learned the details of those incidents "from the FBI" with whom it's cooperating. He declined to provide further details about the other companies or the FBI activities. Donley indicated that investigations underway by the San Antonio police, as well as the FBI, have identified suspects and that "arrests are expected soon."

He declined to provide further details about the investigations or identities of the suspects except to say they included a high school student and an unspecified group of adults who were part of what he described as an "elite" group of UNIX-knowledgeable programmers. Donley said a "UNIX security conference" was held in San Antonio the same week the first hack-attack occurred and that investigators are pursuing the possibility that some conference participants may have engineered the attack on local ISP servers as "an object lesson "in server security flaws. He said that shortly after the newspaper was certain it had been hacked, it offered a reward of $25,000 for information leading to the arrest of the culprits.

He said "we expect to pay it," indicating that the reward offer had already produced information useful to local police and the FBI.

Donley said that seven weeks after the Express-News' service suffered the attack that closed down both its ISP business and its Web site, its systems were still not fully repaired. "We have 300,000 pages on our Web site and as far as we can determine, every one of them was screwed up so that we've had to go through it level by level" he explained. He said a complete financial assessment of the total financial damages and losses caused by the disaster was underway.

The newspaper has taken emergency measures to install new, high-level fire wall systems to insulate its online operations from other internal computer networks, including the one that connects to the headquarters of its parent, Hearst Newspapers.

He said investigations determined that hackers inserted the first destructive programs into the ISP's UNIX server on April 13. The corrupting code soon spread throughout the UNIX Web site files as well.

But the event he characterized as "explosion day" didn't happen for another week. Then, suddenly, none of the assigned system's passwords worked for either inside operators or the ISP's customers. Attempts to use ISP accounts resulted in a notice that the user' had entered an invalid password. Then other functions began to go haywire.

"At first, we thought MIS had screwed up again-that it was an internal problem," said Donley. However, technicians soon discovered havoc throughout the system's code structures and responses. Crucial functions had been diabolically reprogrammed by the invaders. For instance, whenever the command to call up an individual UNIX file was entered, that file was actually deleted. Both the ISP and Web site soon crashed, their structures destroyed.

Editor & Publisher, Vol.130, No.26

Hacker’s Paradise:
Get Wealthy Legally By Cracking A C

By Rodney Ho
Staff Reporter of The Wall Street Journal

A start-up company would like you to hack your way to $1 million.

Crypto-Logic Corp. of Austin, Texas, claims to have created an encryption system for electronic mail so foolproof that it can't be broken. If someone can figure out a special encrypted e-mail message within a year, the company says it will pay a reward of $1 million.

But wait. The technology Crypto-Logic is using for the contest hasn't exactly been foolproof. The three computers needed to create the contest's Web site unexpectedly scrambled data in the site last week, said David Neeley, vice president and chief operating officer.

The breakdown forced him to backtrack from last week's announcement that the contest would begin last Friday. Instead, he spent several days attempting to fix the computers, but to no avail. On Monday, he had to get replacement computers. "I've got thousands of dollars worth of machinery that's not worth blowing up," he grouses. But he adds, "I regard this as my screw-up. In this world, there are no excuses." He finally got the contest running Wednesday, at "http://www.ultimateprivacy.com"

On the bright side, cryptologists agree that the decades-old encryption method that Crypto-Logic is claiming to use -- called a "one-time pad" – is theoretically unbreakable. Each "pad" has a set of uniquely random digital symbols that are coded to the actual message. The recipient uses the same symbols to decrypt the message. The pads are used only once.

To limit the possibility of leaks, Crypto-Logic Chairman Stan Spence is the only person who knows the message that was encrypted. The solution is kept in a NationsBank vault in Austin, Mr. Spence says. In addition, Mr. Neeley says the $1 million is backed by an insurance company he won't name.

Several other companies have held similar contests, typically offering more modest sums.

Jim Bidzos, president of RSA Data Security Inc. in Redwood City, Calif., says his company frequently holds break-the-code contests to test how tough certain encryption systems are. But he and other security experts are skeptical of Crypto-Logic's assertions. "Anyone who says their system is bulletproof is either a liar or stupid," says Winn Schwartau, a Largo, Fla., security expert.

Mr. Neeley admits his integrity is on the line. "If I'm wrong," he notes, "we're out of business."

Teen hacker breaks into Internet files: 16-year-old computer whiz gains access to e-mail

The Ottawa Citizen
Tue, Jun 17 1997

A teenage computer whiz and four of his friends have caused a serious flap after hacking into the e-mail of 1,300 customers of a Brockville-area Internet provider.

Using a computer at his school last Tuesday, the 16-year-old managed to access RipNet for user names and passwords. A number of copies were printed and the group handed them to friends.

``It happened at 10:46," RipNet systems manager Kingsley Grant said yesterday. ``By 2:35 we knew who it was from his log-on and how many times the list had been downloaded to distribute to his friends."

RipNet officials waited until the police had completed an investigation, deciding not to press charges but leaving punishment in the hands of the school. On Friday morning, an e-mail was sent to every affected member advising them to call in for their user names and passwords to be changed.

RipNet is owned by the Brockville Recorder and Times. It has 1,700 members, mostly in Brockville and Smiths Falls.

``So far, all our customers have been superb. They are happy it has been taken care of and that they were notified quickly," said Mr. Grant, who emphasized that no material -- financial or personal -- had been exposed other than e-mail sent or received.

Certainly the punishment handed down by the boy's school, Brockville Collegiate Institute, appears to fit the crime.

``The kid's parents have just left me," Mr. Grant said late yesterday. ``They said their son had been suspended from the school computer room for one year and he had been the highest scoring student in the class for the last two years. He was hoping for a future in computers so it's definitely a serious blow for him.

``His parents ... said he is sick in bed because he is so upset about losing the chance to be in computers next year."

All five boys have been suspended from computer classes next year and must write essays on why what they had done was wrong.

German Hacker Cracks Munich Airport,

According to reports filtering out of Germany over the weekend, a well-known computer hacker known as "Kimble Schmitz," has been extending his electronic world into the real one, and has successfully "hacked" his way past physical security at Munich Airport.

The 23 year-old is reported to have simply knocked on the gatekeeper's door to the airport in the dead of night, and gained admission from a smiling gatekeeper who apparently waved him through.

Schmitz's escapades appear to have been prompted by Focus, the German news magazine, which reported earlier this year that security at Munich Airport was not all it might be. Schmitz has investigated and concluded that security is almost non-existent

Schmitz claims that he first gained access to the airport in May of this year in the small hours of the morning, by posing as owners/travelers on VIP jets in a luxury Mercedes. After the gatekeeper waved them through, he and an accomplice had unrestricted access to the VIP jet area, and, by driving through a second barrier, had access to the national and international jets.

The next day, to test their system, Schmitz and his colleague drove up to the gate during daylight hours, displaying a visitor card from Dataproject, his computer consultancy firm. The security man was apparently fooled by the visitor cards, which can be purchased from most stationery outlets, Newsbytes notes.

According to Schmitz, he and his colleague were able to gain access to the airport tower, where they chatted with staff.

The pair were only caught out a few days later when they made their third visit to the airport, but Schmitz claims that they were stopped when they made the mistake of leaving the airport through a different gate than they entered.

Schmitz, however, had video-taped his escapades, and now the German media is on the warpath. Munich Airport has started a damage limitation exercise with the media and is claiming that, while its own security is not at fault, the lax security on the gate may be due to failure of transfers of responsibility between the airport and the airline.

In retaliation, Munich Airport is reported to have started legal action against Schmitz, claiming trespass. The media, however, seems to be coming down on the side of Schmitz, pointing out that, far from prosecuting the computer consultant, they should solve their own security problems.

Newsbytes notes that this case, if Munich Airport decides to push its claims through the German courts, could get a lot bigger. Whatever happens, it looks as if the management at the airport need to take a crash course in dealing with the media. They will certainly need it as this case continues to grow.

Europe's Hackers Have Come a Long Way Discovers Annaliza Savage

More than 2,000 hackers from around the world turned up at a campsite near Amsterdam last weekend for the Hacking in Progress (HIP) festival. These modem-wielding mavericks had gathered to pitch tents, exchange ideas and technology, and meet their fellows face to face.

Mornings began with the chirping of birds and the booting up of PCs. One tent held lock-picking classes. In another a group of astronomers had set up telescopes linked to computerized data-tracking equipment. Nights were spent chatting by the campfire while someone beside you played Doom on their notebook computer.

Lectures on computer security, the legalities of hacking, and cryptography were held in the main marquee. There were also smaller, more interactive, workshops. Most were computer related, though I did attend one on how to use a yo-yo. This was made all the more bizarre as the head of the Dutch Computer Crimes Division was sitting next to me.

The public telephones malfunctioned on Sunday and could only be used to dial the emergency services. However if you dialed the Dutch equivalent of 999 you got a dial tone, and could dial anywhere in the world for free. I was assured by the organizers that this was a `programming error' on the part of the Dutch telephone company.

HIP was a follow-up to HEU, Hacking at the End of the Universe, which was held at the same spot in 1993. Not only have the numbers increased since then but the hacker scene has also changed.

One obvious difference was that there were just as many females as males. Among them was Rena Tangens, who has been setting up communications networks in the war zone in the former Yugoslavia. Tangens was handing out software her group has written to make the Net accessible in countries where there are no service providers.

Another difference is that Holland's hacker scene has matured. Much of this is due to access.

In 1993 there were no service providers in Holland. To get on to the Internet you had to hack into university or corporate networks. In 1994 the Dutch hacker group Hack-tic decided to start a public provider for everyone. The project turned into Xs4all, now the fourth largest service provider in Holland.

Rop Gonggrijp, the driving force behind HIP and founder of the now defunct Hack-tic, says: `Hackers from 1993 are now the Internet's technicians; there's no more culture of hackers breaking into systems period.' Felipe Rodriguez, a co-founder of Hack-tic, agrees: `They used to call us criminals. Now we advise the Ministry of Justice. We're the only ones who know the technology.' When Rodriguez started there were no laws in Holland against hacking. He believes hackers have been a great asset to systems administrators. `From the moment hacking became illegal, systems became more insecure. The hacker has stopped but the criminal doesn't care about the laws.' HIP proves that the European hacker scene is still active.

Things may have changed, but Gonggrijp thinks the new diversity is positive: `The scene is now pockets of culture. There's alternative media, old hacker culture, UNIX hackers, even astronomers with their own computer culture. It's now for all of the people - we have progressed.'.

GUARDIAN 14/08/97 P4

Cyber Promotions Password
File Posted Online

OTC 8/7/97 7:19 AM

TOKYO, JAPAN, 1997 AUG 7 (Newsbytes) -- By Martyn Williams. For the second time, the complete user name and password file of Cyber Promotions, a company that specializes in mass commercial e-mail, has been posted to Usenet. The file also includes some e-mail addresses and telephone numbers of customers and details of the other domains the company supports and was believed to have been put online by a hacker in protest of Cyber Promotions work.

The file, 931-kilobytes in size, was posted to alt.2600, news.misc and alt.kill.spammers and begins with the complete list of users, passwords, and, in some cases, their e-mail addresses and telephone numbers.

The list continues with details of all the domain names that Cyber Promotions hosts or supports. These include other commercial sales domains, such as answerme.com, cheapcalls.com and savetrees.com but also some more sinister domains including many sex-related sites, such as slutpics.com, nudeteens.com and oralsexpictures.com, and one that deals in hate-speech, godhatesfags.com.

The message was posted to Usenet via a University of Michigan account with the disclaimer, "Once again, I would like to say that the owner of this account had nothing to do with this posting."

At the header of the message, after the disclaimer, the poster addressed readers, "Hi-diddily-ho neighbors! It's me again. Miss me? I missed you too," it began. The message then referenced previous time the passwords were posted and mentioned Sanford Wallace, the operator of Cyber Promotions. "As I assumed, Mr. Wallace has not learned his lesson from the last time I talked to you, so I decided to go a bit father this time, post up more information, from more systems, and a little bit of news on what that low-life degenerate, festering pile of goo is doing in front of his keyboard, behind your backs, right under your noses."

After criticizing the work of a couple of groups in the unsolicited commercial e-mail business, the writer continued, "So, for the news. Here's a ton of new files, including password files for the main system, the http://www.cyberpromo.com web server, and their Nameserver. I also have included their named.boot file and their entire set of DNS zone files."

"You'll note, for example, that Sanford provides nameservice for and hosts the ever-popular "godhatesfags.com" domain. I'm sure you can think of something to do with them all. Not that I would condone any type of illegal activity."

Regarding the hacking and altering of Web sites using the supplied passwords, the writer says, "Which brings me to the point of those of you who decided to make changes to Mr. Wallace's web pages - please, PLEASE clean up after yourselves. If you can't clean up, you probably should just leave it be, as you will get caught."

The Cyber Promotions Web site appears to be none the worse for the exercise. When checked late on Wednesday night the site appeared to be as normal.

Before closing the writer also issued a warning to Netcom, telling them that Cyber Promotions has a script that check's Netcom's finger server every ten minutes looking for new e-mail address to add to the database. "Netcom is a complete waste of bandwidth and I can't stand them and their users for the most part, but some of them are actually cool, and deserve SOME sort of notification of what that sleazebag is doing to them," he said.

In closing, the message said, "Well, I'd say that wraps the whole thing up. Sanford Wallace uses the same password on every machine, and the same root password as his regular password. Guess he has no admin. What a class operation. Not exactly rocket science. His userid is wallace, with a Password of "sTUv6x8r". Guessed the root password yet? Go knock yourselves out."

(19970807/Reported By Newsbytes News Network: http://www.newsbytes.com)